J. Glob. Innov. Agric. Soc. Sci., 2014, 2(3): 143-151.
ISSN (Online): 2311-3839; ISSN (Print): 2312-5225
DOI: 10.17957/JGIASS/2.3.597
http://www.jgiass.com

IMPLEMENTATION OF SOME ENHANCEMENTS IN WIRELESS NETWORK SECURITY BY FINDING VULNERABILITIES, THREATS AND ATTACKS

Muhammad Zaman*[1], Jawad Ahmad[2], Maryam Azhar[3], Arif Nawaz[4], Sammar Abbas[5] and UmerIdrees[6]

Department of Computer Science, University of Agriculture, Faisalabad, Punjab, Pakistan
Corresponding Author's e-mail: zamannazeer@yahoo.com

Due to ease of installation, cost efficiency, scalability and mobility the Wireless networking technology is being deployed everywhere in our daily routine life. With all these advantages WLAN also has security threats and vulnerabilities. Wireless security is necessary to measure, detect and prevent those threats and vulnerabilities. Network security is not only a security threat issue but it is basically a management issue. In this paper some most common types of security threats and vulnerabilities has been discussed and then relevant security policies are being concerned which are implementable to secure the network of any organization or company. This paper also helps normal home users and Security Managers to understand and assess the various threats while using wireless networks and the solutions for countering those threats.
Keywords: WLAN, Security Attacks, Threats, Vulnerabilities, Wireless Security

INTRODUCTION

Wireless networking technology is most popular technology now a day's which connects two or more devices without cables using high frequency radio waves. This gives user facility to move within local coverage area. With a lot of advantages it pose an additional security challenges compared to wired networks. Wireless radio signals propagate through air and are easier to intercept. This introductory section discuss WLAN's Technology, Components and Architecture.

Wireless local area network: A Wireless Local Area Network (WLAN) is a type of local area network that uses high frequency radio waves[1] rather than wires to communicate between network-enabled devices. The first WLAN standard IEEE 802.11 was implemented in 1997 based on Radio technology in the 2.4 frequency with maximum 1 to 2 Mbps throughput. Each device connected in WLAN's called Station. There are two types of stations Access Point and Clients.

WLAN'S Components: All the devices connected in wireless network are called Stations, these are defined in two categories

Access point: Access Point is a hardware device (Wireless Router) that allows wireless communication. Usually, an AP connected to a wired network, and provides signals to connect the mobile devices, Laptops, PDAs to a wireless network.

Client: Client is a hardware device that receives signal from the Access Point (AP) and make connection for the communication like Mobile devices and Laptops connected with router (AP) are called as clients.

WLAN'S architecture: WLAN standard IEEE802.11 has two basic architectures for the communication network as mentioned below:-

AD HOC WLAN: Ad hoc WLAN mode is topology or structure defined in IEEE 802.11 standard. In Ad hoc WLAN's the mobile devices are connected directly in peer-to-peer fashion. It is decentralized network having no pre organized structure like wired networks and access points mounted in other wireless networks. Any device present in coverage area can connect directly to other device. Not used widely due to link stability issues and the as the number of devices/nodes increase the performance of network decrease.

Fig 1: *.Ad hoc WLAN*

Fig 1 describes the structure of ad hoc WLAN networks. Two devices are connected with each other directly in peer-to-peer fashion. Ad hoc networks are used for temporary connection i.e. two friends can use ad hoc network to share data.

Infrastructure WLAN's: Infrastructure WLAN mode is another topology or structure defined in IEEE 802.11 standard. In infrastructure WLAN's the wireless devices (clients) are connected with central device called Access Point (AP) that is connected with backbone wired network to communicate with each other.

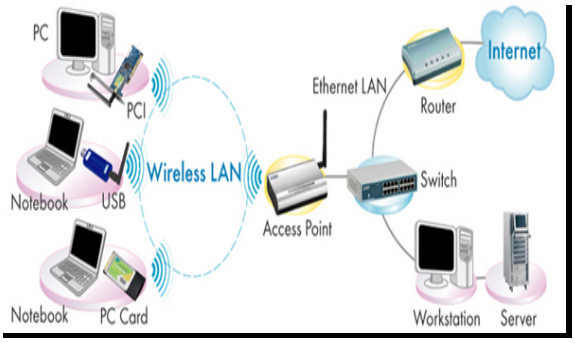

Fig 2: Infrastructure WLAN

Fig 2. describes the structure of Infrastructure WLAN where laptops are connected with wireless Access Point (AP) and AP is connected with wired network through a switch and goes through a router for the internet services. This is used at large number in home, offices and in organizations.

Security vulnerabilities threats & attacks: Ease of installation and low deployment costs make wireless networks attractive to users. However, the easy availability of inexpensive equipment also gives chances to the attackers to learn, practice and find vulnerabilities and to launch attacks on the network. The design flaws in the security mechanisms of the 802.11 standard also give rise to a number of potential attacks, both passive and active. These attacks enable intruders to eavesdrop on, or tamper with, wireless transmissions.

SECURITY VULNERABILITIES

Vulnerabilities can be defined as the weakness in any network that can be exploited by a threat. In simple words the week points in the network from where attacker can attack called vulnerabilities. Recently almost in all areas wireless network technologies have been applied, such as in Banking, Tax, E-Commerce and weak points are also available in wireless communication. Here, followings are some threats and vulnerabilities which are commonly found in the Wireless Network.

Shared Key Authentication Flaw: Shared key authentication can easily be exploited through a passive attack by eavesdropping on both the challenge and the response between the access point and the authenticating client. Such an attack is possible because the attacker can capture both the plaintext (the challenge) and the cipher text (the response).

Service set identifier flaw: access points come with default SSIDs. If the default SSID is not changed, it is comparatively attract more attacks from attackers since these units are regarded as poorly configured devices. Besides, SSIDs are embedded in management frames that will be broadcasted in clear text regardless access point is configured to disable SSID broadcasting or enabled encryption. By conducting analysis on the captured network traffic from the air, attacker is able to obtain the network SSID and performs further attacks.

The Vulnerability of Wired Equivalent Privacy Protocol: Data passing through a wireless LAN with WEP disabled (which is the default setting for most products) is susceptible to eavesdropping and data modification attacks. However, even when WEP is enabled, the confidentiality and integrity of wireless traffic is still at risk because a number of flaws in WEP have been revealed, which seriously undermine its claims to security. In particular, the following attacks on WEP are possible:

1. Passive attacks to decrypt traffic based on known plaintext and chosen cipher text attacks;
2. Passive attacks to decrypt traffic based on statistical analysis on cipher texts;
3. Active attacks to inject new traffic from un authorized mobile stations;
4. Active attacks to modify data
5. Active attacks to decrypt traffic, based on tricking the access point into redirecting wireless traffic to an attacker's machine.

SECURITY THREATS

Threat it can be defined as any person or event that can cause the damage of data or network. Threats can also be natural for example wind, earth quick, lightning, flooding or can be accidental, such as accidentally deletion of file.
Below we discuss some threats and associated losses with their expected growth. The list is not comprehensive some threats may have some common elements to other areas.

Errors and omissions: There are lots of human unintentional errors which contribute in security problems. Sometime a small data entry error can cause the system crash, some of the error occurs during maintenance or installation which can also be a threat for security. Errors are an important threat to the integrity of data. These threads can be produced unintentionally by data entry operators, system operators and developers. People mostly assume that the information coming from a computer system is more accurate. In past few years improvement in software quality reduces this threat.

Fraud and theft: Integrity of data and confidentiality of information are the key features of any system. As information technology is increasing the threat of fraud and theft is also increasing. Attackers use daily new methods to exploit a system, these frauds involve in small amount money to large number of financial accounts. Financial systems are not only the target of hackers, systems which have any resources or controls are under attack by intruders,

For Example University grading system, inventory system, human resource attendance system etc.
Threat of fraud and theft is both from insider or outsider. Majority of frauds are done by the insiders, because they are authorized users and they know the vulnerabilities in the system and they are in better position to commit a crime. Former employees of any organization may also a threat for company if administrators have not terminated their accounts properly and on time.

Physical and infrastructure: This is natural threat, Sometime nature shows its power. It is also a reality that the loss occurs by the cause of natural disasters is more dangerous than viruses, because sometime can cause the damage of whole physical and network infrastructure. Flood, fire, strikes, thunder storm, earthquakes, loss of communication is some of the examples, as we cannot forget the World Trade Center and Tsunami. Sometime these disasters result in an unexpected way. For example in winter storm, even whole computer network is working fully functional but people cannot go to office due to the loss of infrastructure.

Malicious hackers: Anyone who tries to gain illegal access to computer systems for the purpose of stealing or corrupting the data called hacker. Hackers are real and most dangerous threat for the organizations which have big computer system network. They can be from inside the organization, outside the organization or form some other continent. They break the security of the systems, compromise the system and steal the data before any illegal access detected. Hacking can be of two types, ethical hacking and non-ethical hacking. Non ethical hackers are those who are harmful for any organization.

SECURITY ATTACKS

Networks can be attacked from different sources. Attacks can be from two categories: "Passive Attack" when a network intruder intercepts data traveling through the network, and "Active Attack" in which an intruder initiates commands to disrupt the network's normal operation.

Passive attack: These attacks take place for information-gathering silently and are hard to detect. A malicious user just listens to the all incoming and outgoing traffic of a wireless network. Traffic contains packets, and each packet contains juicy information such as packet sequence numbers, MAC address, and much more. Using this attack, a malicious attacker can make an active attack to the network.

Active attack: As the attacker does a passive attack in order to get information about the wireless network, now she/he will do an active attack. Mostly, active attacks are IP spoofing & Denial of Service attack.

IP SPOOFING ATTACKS

IP spoofing is the way that a hacker can hide their own IP and appear his or her IP as someone else IP address. In this attack scenario, the attacker accesses the unauthorized wireless network. Not only that, but also she/he does packet crafting in order to impersonate the authorization of that server or network.

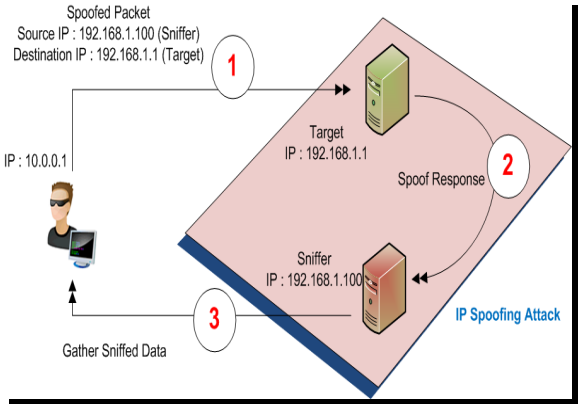

Fig 3: IP Spoofing Attack

Fig 3 describes the how an attacker / sniffer gather the sensitive data by IP Spoofing. In this diagram the hacker creates IP packets targeting a destination, but the source IP field is modified so that it does not have the IP address of the hackers' computer, but in fact, of some other computer, which can be used as a data collector or a sniffer by the hackers.

DENIAL OF SERVICE ATTACK

Here the attacker makes an attack on a particular target by flooding the packets to the server. In most cases, SYN packets are used because they have those capabilities of generating the flood storm.

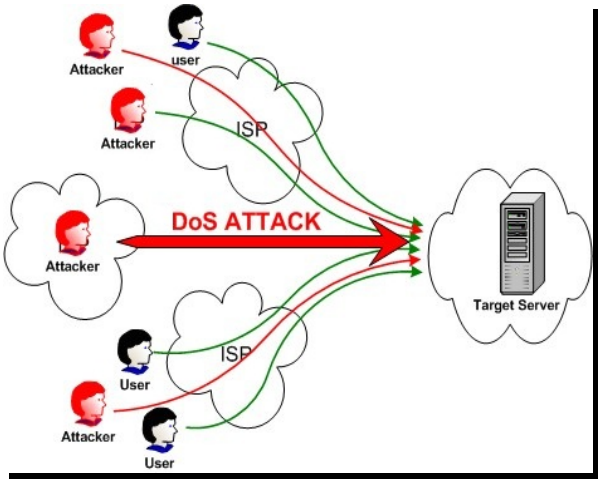

Fig 4: Denial of Service Attack

Figure 4 shows the concept of DoS Attacks. Large amount of requests to a server is difficult to manage. It is based on the server configuration. In the above attack the attacker taking advantage of the server's difficulty. That is sending large amount of requests to the target server in same time .If

these requests become difficult to process to a server, we can say the DoS attack is going on.

MAN IN THE MIDDLE (MITM) ATTACK

Here the attacker accesses the information of the AP of any active SSID. Here dummy APs are created. The attacker listens the communication between to end points. Let's suppose a client is having a TCP connection with any server, then the attacker will be the man in the middle and she/he splits that TCP connection into two separate connections, whose common node will be an attacker himself/herself. So the first connection is from client to an attacker, and the second connection will be from the attacker to the server. So each and every request and response will be taking place between client and server via an attacker. So an attacker can steal information passing in the air between them.

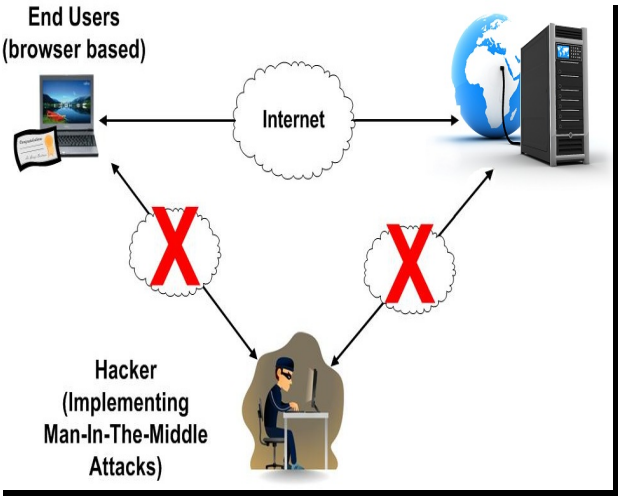

Fig. 5: MITM attack scenario

Fig 5 describes the scenario of man in the middle (MITM) attacks. That two systems are communicating with each other through internet and a third person/hacker interferes between them by taping information. This is such a way that all communication (sending/receiving) takes place through him

PARKING LOT ATTACK

Access points emit radio signals in a circular pattern, and the signals almost always extend beyond the physical boundaries of the area they intend to cover. Signals can be intercepted outside buildings, or even through the floors in multi-story buildings. As a result, attackers can implement a "parking lot" attack, where they actually sit in the organization's parking lot and try to access internal hosts via the wireless network.

Fig 6 describes the signals coverage area of access point (AP) that is exceeding then required area. If a network exceeds required coverage area, attacker has a chance to connect and penetration into the network.

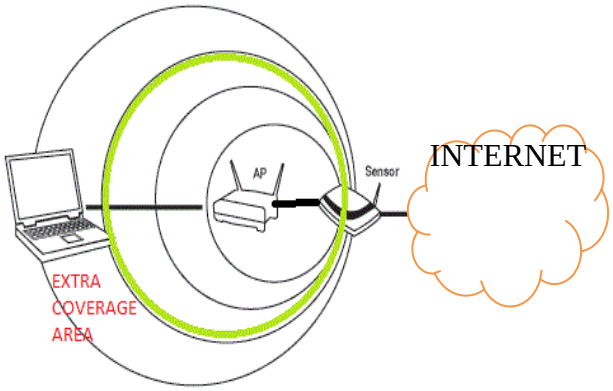

Fig 6: Parking Lot Attack

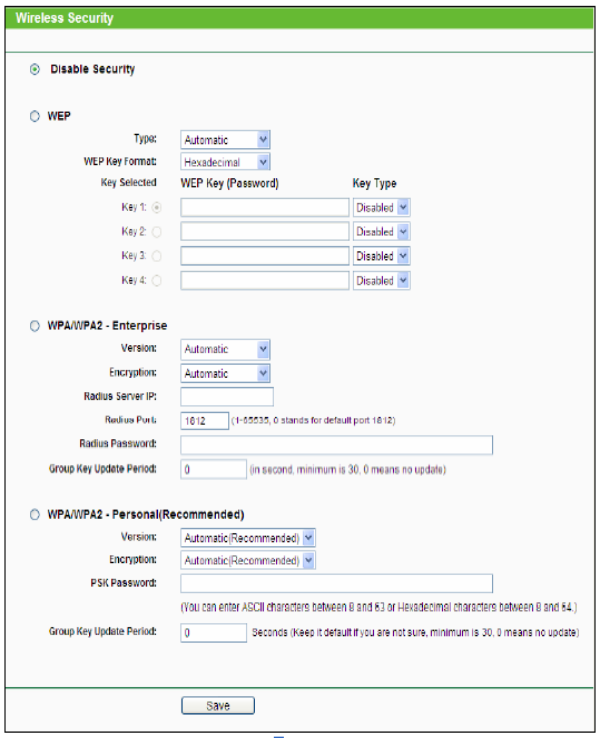

Fig. 7: Implementation of WEP/WPA/WPA2 Security in WLAN

WIRELESS SECURITY

The wireless network protocol architecture has no inbuilt security. Network security system is an essential component[3] of the configuration as well as network management. Implementation of effective network security provides both physical and information security to paths, links, and databases. So techniques such as authentication and encryption are implemented on 802.11 protocols to secure transmission. These techniques[2] are WEP, WPA, and WPA2, respectively known as *"Wireless Equivalent Privacy" &"Wi-Fi Protected Access"& "2"*. Unlike wired networks, a wireless network's signals can be effortlessly intercepted and tampered with. So encryption and authentication is a must for wireless networks. Wireless security is to prevent unauthorized access, threats and vulnerabilities. Some most common types of security policies are following:

Fig 7 shows the implementation setting interface of WLAN according to the user requirement in the TP-Link Router & Access Points. Further detail is as under:-

WIRED EQUIVALENT PRIVACY PROTOCOL (WEP)
Wired Equivalent Privacy (WEP) Protocol is a basic security feature defined in IEEE 802.11 standard, to provide confidentiality over a wireless network by using encryption scheme. But now it is unsecured due to scheduling flaw, because a WEP key can be cracked in a few minutes with some cracking tools. Therefore, WEP should not be used unless a more secure method is not available.

WI-FI PROTECTED ACCESS (WPA)
Wi-Fi Protected Access (WPA) protocol designed to address and fix the flaws in WEP. With the new feature TKIP (Temporal Key Integrity Protocol) for data encryption and 802.11x authentication for user authentication. WPA provides higher level of assurance that their data will remain protected. But since November 2008, vulnerability in TKIP was discovered where attacker may be able to decrypt small packets and inject arbitrary data into wireless network. Thus, WPA is no longer considered as a secure implementation.

WI-FI PROTECTED ACCESS 2 (WPA2)
Wi-Fi Protected Access 2 (WPA2), based on IEEE 802.11i, is an advanced wireless security protocol in which only authorized users can access a wireless device, WPA2 supports strong cryptography AES (Advanced Encryption Standard), strong authentication control EAP (Extensible Authentication Protocol), key management, replay attack protection and data integrity.
TKIP was designed to use with WPA while the stronger algorithm AES was designed to use with WPA2. Some devices may allow WPA to work with AES while some others may allow WPA2 to work with TKIP. New deployments should consider using the stronger combination of WPA2 with AES encryption.

FIREWALL
A firewall is a hardware or software system that prevents unauthorized access to or from a network. They can be implemented in both hardware and software, or a combination of both. The firewall built into router prevents hackers on the Internet from getting access to your PC. But it does not stop people in range of your Wi-Fi signal from getting onto your network but we can secure Personal Computer (PC). But in organizations Firewall used in networks to builds bridge to make external traffic secure coming into the internal network as shown in fig.
Fig 8. Describes the usage of firewall in network for filtering the specific traffic whether they should be allowed through or not by analyzing the data packets based on the preset rules and policies to avoid the hackers, cracker and intruders. Firewall builds bridge between internal and external network and protects internal network or computer.

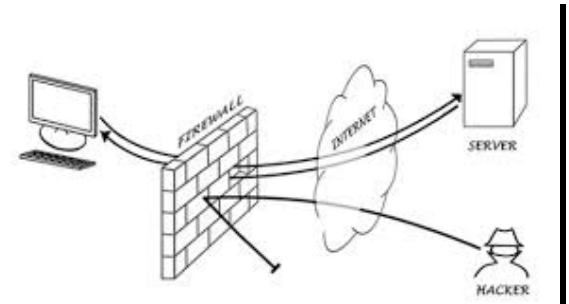

Fig 8: Firewall in Network

INFORMATION PROCESSING IN A CORPORATE ENVIRONMENT
The adoption of wireless networks in the corporate environment has been on the increase. Many small and medium enterprises have switched to wireless networks, due to the ease of installation and low cost of wireless devices. However, convenience and flexibility come at a price; the security threat level increases with the use of wireless networks due to the inherent characteristics and weaknesses of wireless network protocols. Therefore, it is important to examine the applicability of wireless networks for information processing in a corporate environment.
The following Categories of information are defined with respect to the transmission of information in accordance with the requirements specified in the Security Regulations[4].

TOP SECRET
This information is classified as Not Allowed category from all sides.

SECRET
This is also categorized as Not Allowed.

CONFIDENTIAL
Allowed, with the authentication and transmission encryption security controls. Use of a VPN is recommended to provide a strong authentication and encryption tunnel over a WLAN connection. In addition, proper key management and configuration policies should also be established to complete the technical solution.

RESTRICTED
Allowed, with the same level of encryption and authentication and required for CONFIDENTIAL information is recommended, using proper key management and configuration policies.

UNCLASSIFIED
Allowed, similar to the specifications for CONFIDENTIAL and RESTRICTED information, proper key management and configuration policies should be established to complement the technical solution.

WIRELESS SECURITY DEPLOYMENT
To tackle vulnerabilities, threats, risks and attacks

effectively, various security best practices need to be considered throughout the entire deployment lifecycle. To help organizations understand at what point in their wireless network deployments a recommended security, we outline here a five-phase lifecycle model for network deployment and point out security issues that need special attention.

INITIALIZATION PHASE

Requirements for the Use of the WLAN: Before designing the wireless network, it is important to understand the business and functional requirements of the wireless solution. These can make affective decisions that what kind of security measures should be deployed to protect the network.

Define a Wireless Security Policy: The organization should develop a strong wireless security policy for the development of installation, protection, management and usage procedures. Security and operation guidelines, standards and personnel roles should also be clearly defined.

DESIGN PHASE

Keep Track of Development for Wi-Fi Standards: Since the 802.11 standard was first introduced, enhancements have continuously been made to strengthen data rates, signal range, and security of wireless networks. Therefore, it is a good idea to keep track of the development of new standards as they appear, particularly when acquiring new wireless network equipment and services.

Perform Security Risk Assessments and Audits: Security assessments and audits are essential means for checking the security status of a wireless network and identifying any corrective action necessary to maintain an acceptable level of security. These assessments can help identify loopholes in the wireless network, such as poorly configured access points using default or easily guessed passwords and the presence or absence of encryption.

Perform Site Surveys: Due to the nature of radio frequency (RF) propagation, radio signal emissions cannot generally be contained within a particular building or location. Excessive coverage by the wireless signal could pose significant threat to the organization, opening it to parking lot attacks on the network. Therefore, it is necessary to have a good understanding of the coverage requirements for the desired wireless network during the network-planning phase. By performing a site survey, one can identify:

1. the appropriate technologies to apply;
2. obstacles to avoid, eliminate, or work around;
3. coverage patterns to adopt

Apply a defense-in-depth approach: The concept of "defense-in-depth" has been widely employed in the secure design of wired networks. The same concept can also be applied to wireless networks. By implementing multiple layers of security, the risk of intrusion via a wireless network is greatly reduced. If an attacker breaches one measure, additional measures and layers of security remain in place to protect the network.

Separation of wireless and wired network segments, use of strong device and user authentication methods, application of network filtering based on addresses and protocols, and deployment of intrusion detection systems on the wireless and wired networks are all possible measures that can be employed to build multiple layers of defense.

Separate Wireless Networks from Wired Networks: Due to the nature of wireless technology, wireless networks are relatively hard to contain within a building and it is generally considered to be an un-trusted network. As a best practice, wireless networks and wired networks should not be directly connected to each other. It is common to deploy firewalls to separate and control the traffic between different networks. For example, ARP broadcast packets should be blocked from entering a wired network from a wireless network since a malicious user could uncover internal information, such as Ethernet MAC address from these broadcasts.

IMPLEMENTATION PHASE

Many different possibilities and ways to make to secure WLAN,s can be considered some of them valuable ways and techniques are following [7]

Physical security controls: Implement strong physical security controls because, the loss or theft of network equipment can be a significant threat to a wireless network and to the organization because configuration of the network can be retrieved from that lost access point. We can minimize this risk of theft by mounting network devices and equipment securely, such as access points should be mounted in less accessible locations together with strong physical security controls.

Fig. 9: Physical Security

Figure 9. Describes the physical security of access point (AP) or other devices that all devices should be mounted safely and at secure place.

Avoid excessive coverage of wireless networks: The excessive coverage of wireless network provide chances to intruders, we can limit it with limiting the coverage of wireless networks by proper placement of access points. In addition to proper placement of the access points, use directional antennas to control the propagation of the (radio frequency) RF signal and hence control coverage of a wireless network only accessible within required region.

Secure access points: Access points are the core of a wireless network and it should not be accessible to unauthorized user. Their security clearly has an overall effect on the security of the wireless network. Properly securing access points is the first step in protecting a wireless network. The following suggestions can help in hardening access points:

1. Change the default configuration settings.
2. Change encryption keys regularly.
3. Ensure that all access points have strong, unique administrative passwords and change the passwords regularly.
4. Disable all insecure and unused management protocols on access points and configure the remaining management protocols for least privilege.

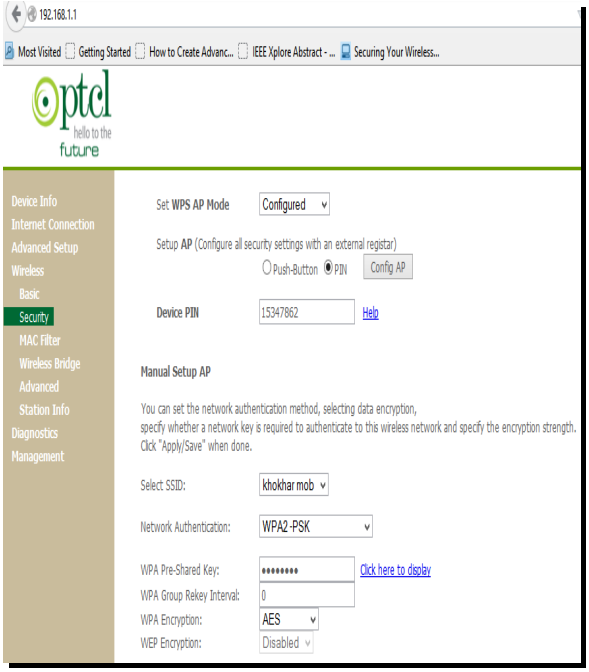

Fig 10: Securing Wireless Access Point

Fig 10. Describes the configuration of SSID on PTCL router, we can simply login by browsing 192.168.1.1 default address and giving ‘admin’, ‘admin’ user name and password and after that go to security and set SSID , Authentication, Encryption and Security Key.

Use Non-suggestive Service Set Identifier (SSID) Naming Conventions: In a wireless network, an SSID serves as a network name for segmenting networks. A client station must be configured with the correct SSID in order to join a network. The SSID value is broadcast in beacons, probe requests and probe responses. To prevent a malicious attacker from collecting reconnaissance information on a wireless network by eavesdropping, SSIDs should not reflect internal information of the organization.

MAC Address Filtering on Access Points: MAC address filtering can be considered the first layer of defense for wireless networks. With MAC address filtering enabled, only devices with pre-approved MAC addresses can see the network and be granted access to the network. However, such access control should by no means be solely relied upon to protect data confidentiality and integrity, as tools are available on the Internet for modifying the MAC address of a client. Besides, MAC address filtering mechanisms may not be feasible in some scenarios such as the implementation of public wireless hotspots.

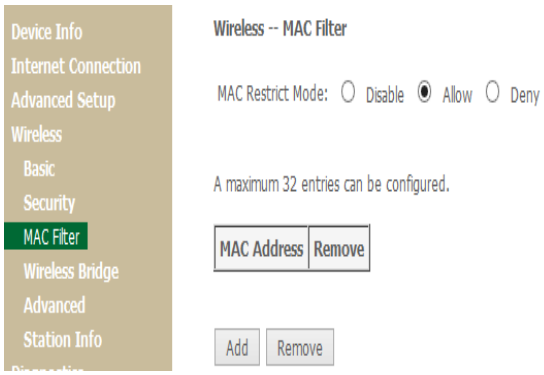

Fig. 11: MAC Filtering

Fig 11describes the MAC address filtering to allow only the preset and allowed MAC address devices, in ALLOW option added MAC address will be allowed and the MAC addresses added in DENY option will not be able to connect

Disable Direct Client-to-Client “Ad-Hoc Mode” Transmissions: In general, a wireless network can be operated using three different topologies; infrastructure mode, ad-hoc mode and bridging mode. When a wireless network operates in ad-hoc mode, client stations are connected directly and no access point is required. Using this mode, a potential attacker can gain access to a client station easily if the client station is improperly configured. Unless there is a specific business need, the ad-hoc mode should be disabled on wireless devices.

Limit Client-to-Client Communication through the AP: Most installed wireless networks operate in “infrastructure” mode that requires the use of one or more access points. With this configuration, all traffic in the wireless network travels through the access points. By controlling the communication among client stations at the access points, malicious users can be prevented from gaining access to vulnerable client stations.

Deploy Wireless Intrusion Detection Systems: Deploying wireless intrusion detection systems on the network can help detect and respond to malicious activities in a timely manner. More recently, a number of wireless intrusion detection systems have been equipped with capabilities to detect and prevent rogue access points.

OPERATIONS AND MAINTENANCE PHASE

Educate users about the risks of wireless technology: User awareness is always a critical success factor in effective information security. A good policy is not enough. It is also important to educate all users in following the policy. Best practices or security guidelines should be developed that end-users understand and adhere to.

Keep an accurate inventory of all wireless devices: An accurate inventory of all authorized wireless devices helps identify rogue access points during security audits. This inventory will also be helpful for a variety of support tasks.

Publish a coverage map of the wireless network: Network administrators should develop a coverage map of the wireless network, including locations of respective access points and SSID information. This map is a valuable asset for troubleshooting, or handling a security incident.

Develop security configuration standards for access point: To simplify daily operations and ensure all access points are protected with appropriate measures, it is recommended a baseline security configuration standard for access points be developed. It is not uncommon to see security settings restored to their default factory settings after an access point is reset, which usually occurs when the access point experiences an operational failure. If a baseline security configuration standard is available, appropriate personnel can simply follow the standard settings to re-configure the access point.

DISPOSITION PHASE

Remove all sensitive configuration information before disposal: During disposal of wireless components, it is important to delete/clear all sensitive configuration information, such as pre-shared keys and passwords, on the devices that are being disposed of. Malicious users might make use of the configuration information to conduct subsequent attacks on the network. Manual removal of configuration settings through the management interface is a must prior to disposal.

CONCLUSION

The aim of this paper was to explore the wireless network vulnerabilities, threats and different security attacks and their countermeasures. Security of wireless network is not just password enabling it's properly placement of devices and then their configuration with strong passwords that should be changed on regular basis and the security policies and standards as mentioned in the paper which is really helpful for making home, office or any organization wireless transmission/ communication confidential over the air. If a user or an organization implements a wireless network according to aforesaid technical measurement then that organization can be avoid the different types of network security threats and attacks.

REFERENCES

Broch, J., Maltz, D.A., Johnson, D.B., Hu, Y. and Jetcheva, J., "A performance comparison of multi-hop wireless ad hoc network routing protocols", in MobiCom '98: Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking, 1998, pp. 85-97.

Gerla, M., Hong, X. and Pei, G., "Landmark routing in ad hoc networks with mobile backbones", in Journal of Parallel and Distributed Computing, vol. 63, no. 2, pp. 110-122, February 2003.

Viana, A. C., de Amorim, M. D., Fdida, S. and de Rezende, J. F., "Indirect routing using distributed location information", in PERCOM '03: Proceedings of the First IEEE International Conference on Pervasive Computing and Communications, 2003, pp. 224

J. Eriksson, M. Faloutsos and S. Krishnamurthy. "DART: Dynamic Address RouTing for Scalable Ad Hoc and Mesh Networks". in IEEE- ACM Transactions on Networking, vol. 15, no. 1, April 2007, pp. 119-132.

Alvarez-Hamelin, J.I., Viana, A.C.; De Amorim, M.D., "Architectural Considerations for a Self-Configuring Routing Scheme for Spontaneous Networks", in Technical Report, vol. 1, October 2005, pp. 1.

[6] Caleffi, M., Ferraiuolo, G., and Paura, L., "Augmented Treebased Routing Protocol for Scalable Ad Hoc Networks", in MHWMN '07: Proceedings of the Third IEEE International Workshop on Heterogeneous Multi-Hop Wireless and Mobile Networks, 2007.

Lee, S.J., and Gerla, M., "Split Multipath Routing with Maximally Disjoint Paths in Ad Hoc Networks", in ICC '01: Proceedings of the IEEE International Conference on Communications, pp. 3201-3205, 2001

Ball., M.O., "Complexity of network reliability computations", in Networks, vol. 10, no. 2, 1980, pp. 153-165. [9] Lin, H., Kuo, S., and Yeh, F., "Minimal cutset enumeration and network reliability evaluation by recursive merge and BDD", in ISCC '03: Proceedings of the 8th IEEE international Symposium on Computers and Communications, 2003, pp. 1341-1346.

Valiant, L.G., "The complexity of enumeration and reliability problems", in SIAM Journal of Computing, vol. 9, 1979, pp.410-421.

The VINT Project. "The ns Manual (formerly ns Notes and Documentation)".

Bai, F., Sadagopan, N., Krishnamachari, B., and Helmy, A., "Modeling path duration distributions in MANETs and their impact on reactive routing protocols", in IEEE Journal on Selected Areas in Communications, vol. 22, no. 7, 2004, pp. 1357-1372.

Multicast Lifetime Maximization for Energy-Constrained Wireless Ad-hoc Networks with Directional Antennas Song Guo and Oliver Yang CCNR Lab, School of Information Technology and Engineering University of Ottawa, Ottawa, Ontario, Canada.

Trading Latency for Energy in Wireless Ad Hoc Networks using Message Ferrying Hyewon Jun, Wenrui Zhao, Mostafa H. Ammar, Ellen W. Zegura, and Chungki Lee College of Computing, Georgia Institute of Technology , Atlanta, Georgia

Stability Oriented Routing in Mobile Ad-Hoc Networks Based on Simple Automatons ByMiklosMolnar and Raymond Marie University of Montpellier 2, IUT / LIRMM University of Rennes France

Routing in Mobile Ad Hoc Networks By Fenglien Lee University of Guam Guam, US.